Gartner Research

2025 Cybersecurity Primer: Build and Optimize Cybersecurity Programs

Mary Ruddy

29 January 2025

Gartner®

2025 Cybersecurity Primer: Build and Optimize Cybersecurity Programs

29 January 2025 - ID G00822280 - 12 min read

By: Mary Ruddy

Initiatives: Build and Optimize Cybersecurity Programs

Delivering effective cybersecurity initiatives helps cybersecurity leaders balance the dual role of protecting the organization and delivering business value in constantly shifting threat and operating environments. One of three key needs is to build and optimize a cybersecurity program.

Scope

Use the cybersecurity initiative to build and optimize an overall cybersecurity program, which includes cybersecurity strategy, technical infrastructure and organizational structure.

Topics in this initiative include:

- **Define Vision, Strategy and Operating Model:** Determine a vision, a strategy and an operating model that can succeed in today's distributed, fast-changing environment.
- **Design and Optimize Security Tools and Services:** Select, deploy and run the security products and services that will help your organization mitigate the right cybersecurity risks and enable zero trust.
- **Secure Applications and Data:** Enable secure innovation by protecting data and applications.
- **Source, Develop and Retain Talent:** Develop a strategy to source, develop and retain talent on your team.
- **Assess and Manage Cyber Risk (Including 3rd Party Risk):** Enable your organization to manage cyber risks related to privacy, safety and reliability.

- **Enable and Protect AI:** Enable organizational AI strategy through proactive governance, risk management and cybersecurity innovation.

- **Optimize Identity and Access Management:** Manage and optimize an overall IAM program to support identity-first security and zero trust.

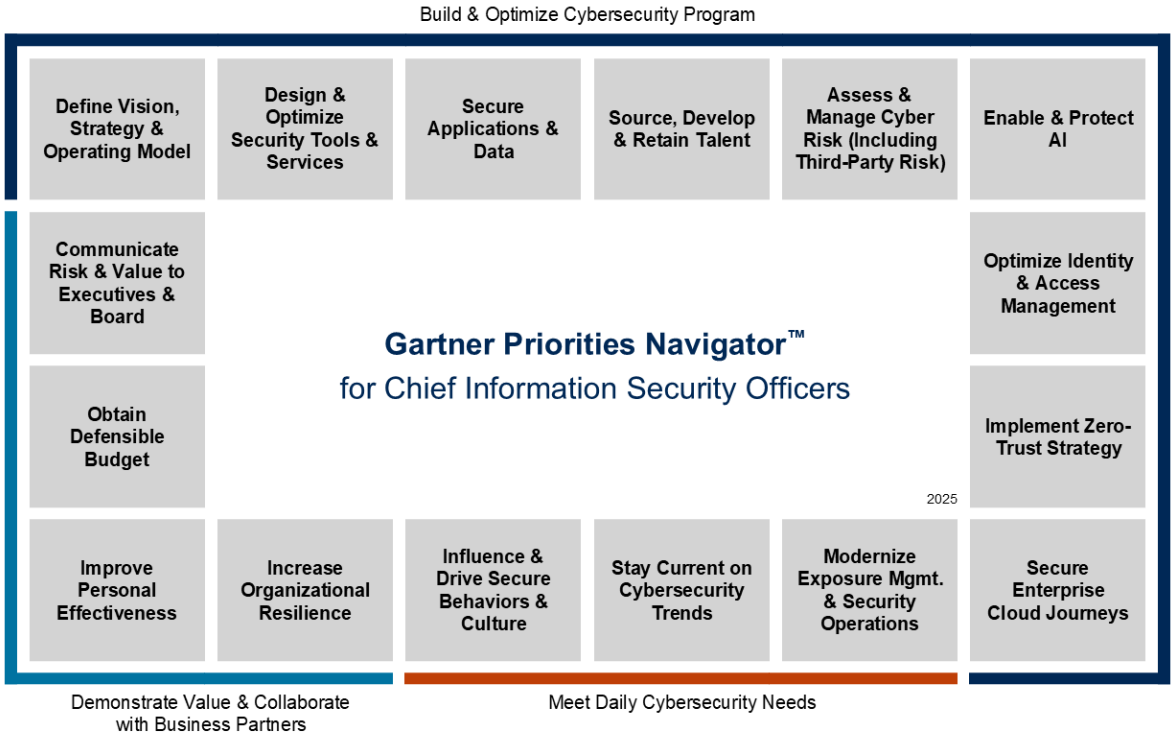
- **Implement Zero-Trust Strategy:** Architect and deploy an effective zero-trust implementation.

- **Secure Enterprise Cloud Journeys:** Design and implement security in cloud deployments from the inception of cloud migration plans.

Some content may not be available as part of your current Gartner subscription. Contact an account executive if you wish to discuss expanding your access to Gartner content.

Analysis

Figure 1: Gartner Priorities Navigator for Chief Information Security Officers



Source: Gartner
822280

Gartner

This initiative is the first in a set of three designed for cybersecurity leaders:

1. 2025 Cybersecurity Primer: Build and Optimize Cybersecurity Programs
2. 2025 Cybersecurity Primer: Meet Daily Cybersecurity Needs
3. 2025 Cybersecurity Primer: Demonstrate Value and Collaborate With Business Partners

Rapid change continues to put pressure on cybersecurity leaders and their teams. Use of AI technologies holds the promise of improving productivity, but brings new challenges and risks of its own. Cyberthreats are proliferating. Digital assets are growing in both number and type, and are more distributed and subject to more frequent change, which can require additional security approaches. This creates intense pressure to optimize investments, even with a growing budget.

Risk appetites should be adjusted and reviewed continuously. Organizations should balance efforts to manage risk with the imperative to engage more effectively and efficiently with all their user constituencies, including customers, partners and workers. Cybersecurity leaders must adapt their existing programs to create new strategies for addressing cybersecurity risk. A zero-trust strategy is part of an overall cybersecurity strategy for many organizations. Operating models must become more distributed to accommodate changes in how they source and use cybersecurity talent and security and identity infrastructure. Cybersecurity infrastructure must become more resilient, less siloed and more effective at sharing risk signals. Using the cybersecurity mesh architecture (CSMA) approach as a North Star can help. Cybersecurity leaders should plan on operating in an environment of ongoing change.

This initiative will provide cybersecurity leaders with the insights needed to understand the implications of these dynamics. It will help them develop and optimize a cybersecurity program that sustains value creation in a rapidly changing world.

Topics

The first requirement is to build and optimize a cybersecurity program, which should be the cornerstone of an organization's cybersecurity initiatives. The program should encompass many elements, including strategy, operating model, technical infrastructure, talent and risk management. Cybersecurity leaders must evolve their operating models to distribute decision rights and account for rapid change and the further decentralization of IT.

Our research in this area addresses the following topics:

Define Vision, Strategy and Operating Model

In times of rapid change, it is crucial to be clear about your organization's cybersecurity mission and vision. Cybersecurity leaders should revisit their strategic assumptions to ensure these align with their organization's objectives and business drivers. Given rapidly changing threat and operating environments, cybersecurity leaders must evolve their operating models to achieve desired outcomes in a more dynamic and complex world.

Questions Your Peers Are Asking

- How do I develop a coherent vision for our cybersecurity program?
- What are the elements of a cybersecurity strategy, and how do I develop them?
- How are security operating models changing in response to the democratization of IT?
- What is the optimal structure for my cybersecurity team?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Leadership Vision for 2025: Security and Risk Management
- CISO Foundations: How to Design a Practical Cybersecurity Organization
- CISO Foundations: Toolkit — Strategic Planning Presentation and Dashboards
- Tool: Sample Cybersecurity Organization Charts
- Case Study: Nationwide Building Society's Approach to Product-Aligned Cybersecurity

Planned Research

- Aligning cybersecurity leadership with enterprise risk
- Tool: Cybersecurity and Infrastructure Security Agency's (CISA's) zero-trust maturity model
- CISO's starter guide to integrate AI in cybersecurity strategy
- Security fundamentals — The services and processes you must get right
- 6 steps to build a productized security program

Design and Optimize Security Tools and Services

Putting a cybersecurity strategy into practice requires the right tools and their effective implementation. Fulfilling this requirement is especially challenging at a time when organizations are modernizing their infrastructure and finding that legacy approaches clash with digital transformation efforts. Cybersecurity leaders must optimize their tool selection and processes to implement zero-trust principles throughout their organization, and achieve efficiencies in the long term by operating and maintaining them correctly.

Questions Your Peers Are Asking

- How do I identify the tools and services that will help me achieve my strategic goals?
- How should I modernize our cybersecurity architecture?
- How do I maintain a particular security capability?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Magic Quadrant for Endpoint Protection Platforms
- Guide to Network Security Concepts
- Market Guide for Managed Detection and Response
- Reference Architecture Brief: Network Security
- Top 5 Challenges of Microsoft Defender for Endpoint and How to Overcome Them

Planned Research

- A journey guide to building a security operations function
- Cybersecurity mesh architecture 3.0 (CSMA)
- The CISO's guide to quantum computing
- Magic Quadrant for Cyber-Physical Systems (OT) Protection Platforms
- Jump-start your AI security strategy with an AI security platform

Secure Applications and Data

The tools used to protect applications and data need to evolve to meet the needs of AI-based services. As cybersecurity programs mature, risk ownership for applications, data and other technology assets is spread throughout organizations. Security decisions are no longer confined to the security team, but are increasingly made independently by other people across the enterprise. New processes, tools and metrics are needed to collaborate with teams across business units and software engineering, data and analytics, and other functions.

Questions Your Peers Are Asking

- How do I enable teams to implement the appropriate cybersecurity controls?
- How do I identify new business initiatives that require cybersecurity's involvement?
- How do I collaborate with application teams to secure agile or continuous delivery?
- How do I enable teams to secure the organization's data assets?
- How do I get business leaders to "own" cyber risk when their inclination is to view this as the job of cybersecurity or IT teams?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- 4 Steps to Accelerate Adoption of Data Security Governance
- Adapt Your Third-Party API Security to 3 Specific Use Cases
- Market Guide for Data Masking and Synthetic Data
- Streamline Your DevSecOps Profile
- Leader's Guide to Software Supply Chain Security

Planned Research

- Securing unstructured data
- Building a cryptographic center of excellence
- Securing the software supply chain
- Integrating security into the DevSecOps toolchain
- Securing software development environments

Source, Develop and Retain Talent

While demands on cybersecurity leaders and their teams grow, available talent remains scarce. Cybersecurity leaders must, therefore, develop a focused talent acquisition, development and retention strategy. This should include strategic use of outsourcing and external hiring, and the creation of both a pipeline to identify and develop internal or nontraditional candidates and improved practices to retain hard-won talent.

Questions Your Peers Are Asking

- How do I attract, develop and retain talent?
- What roles and skills will I need in the future?
- Where can I outsource to address talent shortages?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Cybersecurity Job Descriptions Library
- CISO Foundations: Cybersecurity Talent Management Strategies
- CISO Effectiveness: How to Attract, Retain and Release Cybersecurity Talent
- CISO Effectiveness: Addressing the Cyber-Physical Systems Security Skills Gap
- How to Prepare for, and Establish, an Effective Identity and Access Management Team

Planned Research

- CISO Effectiveness: Five questions your HR partner must ask cybersecurity candidates
- Tool: Skills and competency assessment to future-proof your cybersecurity workforce
- How to staff a data loss prevention program
- How to staff a security operations center effectively
- Workforce management plan to reduce the impacts of burnout in security operations

Assess and Manage Cyber Risk (Including 3rd Party Risk)

Concerns about cyber risk extend from core IT systems and business-managed software applications to digital connections with third parties. Cybersecurity leaders need to build defensible security programs and use their expertise in risk management to limit and mitigate exposures of cyber-physical systems (CPS), aka operational technology (OT), and the personal data of individual employees and customers. They must also guide their organizations' response to disruptive technologies and increased regulatory scrutiny on cybersecurity practices.

Questions Your Peers Are Asking

- How should I define and build a cyber-risk management program?
- How should I manage third- and nth-party cybersecurity risks?
- How do I facilitate the setup and evolution of a privacy function that's responsive to regulatory and technological developments?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Boost CPS Security With Federated Governance
- The Cyber-Risk Management Cookbook for Security Leaders
- Practical Privacy — Balancing Risk and Value in Data Sharing and Collaboration
- Take a Life Cycle Approach to Managing Third-Party Cyber Risk

- Tool: Third-Party Cybersecurity Risk ManagementPolicy Template

Planned Research

- Hype Cycles for cyber risk management, CPS and privacy
- Buyers' guide for cyber GRC
- How security leaders get more out of cyber-risk quantification
- Tabletop exercise for CPS security
- Trends in privacy

Enable and Protect AI

Cybersecurity leaders must secure how their organization leverages and consumes AI technology and navigate its impacts on security and the organization. Generative AI (GenAI) holds the promise of transformative improvement for a wide range of security and business processes, but CISOs will be accountable for doing this safely and efficiently.

Questions Your Peers Are Asking

- How do we govern and manage cyber risks associated with organizational use of third-party AI applications and embedded AI features in corporate applications?
- How do we adapt application and data security practices to the development of AI and GenAI?
- What are the cybersecurity use cases and benefits of AI and GenAI?
- How should we prepare and respond to threat actors leveraging AI and GenAI?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Use TRiSM to Manage AI Governance, Trust, Risk and Security
- Top 4 Copilot for Microsoft 365 Security Risks and Mitigation Controls
- Use ODMs to Guide Defensible Cybersecurity Investment in GenAI Risk Reduction
- Tool: RFI for Generative AI Model Vendors

- Detect Deepfakes to Guard Against Impersonation and Disinformation

Planned Research

- Predicts 2025: Privacy in the Age of AI and Dawn of Quantum
- Tool: Board briefing on cybersecurity implications of generative AI
- Navigating AI adoption and governance
- How security leaders should prepare for GenAI-augmented social engineering attacks
- Jump-start your AI security strategy with an AI security platform

Optimize Identity and Access Management

Identity and access management (IAM) is a crucial foundation for security in today's distributed digital environment. Protecting against cyberthreats while enabling legitimate users (including customers and machines) requires a flexible identity infrastructure — an identity fabric. Cybersecurity leaders must evolve their IAM services for greater security, resilience, interoperability and ease of use.

Questions Your Peers Are Asking

- How do I set up an IAM program, manage it and measure its effectiveness?
- How should I architect for IAM?
- What are the best practices for IAM?
- How should I manage privileged access for humans and machines?
- How do I minimize account takeover and identity fraud?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Identity-First Security Maximizes Cybersecurity Effectiveness
- Magic Quadrant for Access Management
- Reference Architecture Brief: API Access Control

- 2025 Planning Guide for Identity and Access Management
- Address Top IAM Hygiene Issues to Enhance Security and Reduce Risk

Planned Research

- Best practices for improving IGA access certification outcomes
- Innovation Insight: Enhancing cloud security with cloud infrastructure entitlement management
- How to build an effective IAM team to drive transformation and business value
- IT Score for Identity and Access Management
- Innovation Insight: Adopting IAM journey-time orchestration to optimize UX and mitigate risks

Implement Zero-Trust Strategy

Many cybersecurity programs cite a zero-trust strategy as core to their cybersecurity program. Organizations can further reduce cybersecurity risk by replacing implicit trust with the explicit authentication of each user and authorization of each access. Formulating and implementing a zero-trust strategy requires orchestrating a well-prioritized sequence of activities and a high level of stakeholder engagement.

Questions Your Peers Are Asking

- How do we design a zero-trust strategy and deployment plan?
- What capabilities are needed for practical zero-trust implementation?
- What is the best way to mature our zero-trust implementation?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- Tool: Zero-Trust Conversation Guide for CISOs
- Strategic Roadmap for Zero Trust Security Program Implementation
- How to Build a Zero Trust Architecture
- Use the U.S. DOD Model for Your Zero Trust Approach: User Pillar

- Market Guide for Zero Trust Network Access

Planned Research

- The role of zero-trust architecture in email security
- Strategic Roadmap for Zero-Trust Strategy
- Improving unstructured data security through zero trust
- Three identity ingredients required for zero trust initiatives to succeed
- Voice of the customer for zero-trust network access

Secure Enterprise Cloud Journeys

Security teams are challenged to protect multiple types of cloud deployment at scale. Old mechanisms befitting on-premises deployments are ill-suited to the dynamics of multicloud deployment. In parallel, cloud service providers are enhancing their existing native capabilities and introducing new ones. An automated, self-organizing approach is necessary to provide security enforcement and governance at scale.

Questions Your Peers Are Asking

- How can my teams and I keep up with the rapidly expanding cloud adoption?
- How should I approach security governance for multiple cloud environments?
- How do I determine the risk to my cloud applications?
- Are native cloud security controls enough to protect my deployment?
- How should I protect SaaS, IaaS and PaaS — with native or third-party tools?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- CISO Effectiveness: How to Optimize Your Security Team's Structure for the Cloud
- Guide to Cloud and Infrastructure Security Concepts
- Solution Path for Security in the Public Cloud
- 3 Secure Cloud Journey Essentials for CISOs

- Outcome-Driven Metrics You Can Use to Evaluate CloudSecurity Controls

Planned Research

- Data-centric security for the cloud
- Leaders' guide to cloud security
- How to assess and improve your cloud-native application protection platform (CNAPP) maturity
- How to conduct risk-based evaluation of cloud service provider's security
- Security considerations and best practices for securing serverless PaaS and functions as a service (FaaS)

Suggested First Steps

- IT Score for Security and Risk Management
- CISO Effectiveness: Security Operating Models Are Evolving
- Effective Metrics Practices for Cybersecurity Leaders
- 2024 Strategic Roadmap for Managing Threat Exposure

Essential Reading

- Top Trends in Cybersecurity for 2025
- Leadership Vision for 2025: Security and Risk Management
- CISO Foundations: Build a Defensible and Agile Security Program
- Augmented Cybersecurity: Act Now to Thrive Amid Chaos and Complexity
- 4 Ways Generative AI Will Impact CISOs and Their Teams
- Infographic: Map Your Cybersecurity Controls Performance and Investments
- CISO Effectiveness: Hiring and Developing Nontraditional Cybersecurity Talent

Tools and Toolkits

- Tool: Enterprise Information Security Charter Template
- Tool: Sample Cybersecurity Organization Charts
- Security Project Prioritization Tool
- Tool: Cybersecurity Platform Consolidation Workbook
- Tool: Identifying Adjacent Talent for Key Cybersecurity Roles
- Tool: Third-Party Cybersecurity Risk Management Policy Template
- Tool: Templates for Building an Effective Zero-Trust Strategy

Document Revision History

2024 Cybersecurity Primer: Build and Optimize Cybersecurity Programs - 24 July 2024

2024 Cybersecurity Primer: Build and Optimize Cybersecurity Programs - 31 January 2024

2023 Cybersecurity Primer: Build and Optimize Cybersecurity Programs - 14 February 2023

Related Priorities

Initiative Name	Description
Demo Value and Collaboration With Bus. Partners	Use this cybersecurity initiative to demonstrate value and work with the business. This involves obtaining a defensible budget and communicating both value and risk to the board, C-suite and peers.
Meet Daily Cybersecurity Needs	Leverage Gartner's cybersecurity initiative to meet daily cybersecurity needs. Learn about new threats and security trends to improve exposure management and incident response.

Related Priorities

Initiative Name	Description
Demo Value and Collaboration With Bus. Partners	Use this cybersecurity initiative to demonstrate value and work with the business. This involves obtaining a defensible budget and communicating both value and risk to the board, C-suite and peers.
Meet Daily Cybersecurity Needs	Leverage Gartner's cybersecurity initiative to meet daily cybersecurity needs. Learn about new threats and security trends to improve exposure management and incident response.

Initiative Name	Description
Demo Value and Collaboration With Bus. Partners	Use this cybersecurity initiative to demonstrate value and work with the business. This involves obtaining a defensible budget and communicating both value and risk to the board, C-suite and peers.
Meet Daily Cybersecurity Needs	Leverage Gartner's cybersecurity initiative to meet daily cybersecurity needs. Learn about new threats and security trends to improve exposure management and incident response.